EXPO 2010 SHANGHAI CHINA

IBM

中国2010年上海世博会高级赞助商

企业信息安全管理

全球市场压力对我们大家都有影响

- 我们生活在一个真正实现了全球整合的世界
  - 经济低迷和不确实产生了广泛影响
  - 能源短缺和日用品价格波动
  - 全新客户需求和业务模式
  - 信息激增及风险/机会的增长

- 各机构在有效实现下述目标方面遇到了压力
  - 管理运行成本和复杂性
  - 提供持续的服务可用性和高质量体验
  - 迎接前所未有的安全性、永续性和制度遵从挑战
  - 利用新兴技术来推动业务创新、提高效率及响应性

“过去十年发生的变化，比以前的90年还要猛烈。”

Ad J. Scheepbouwer,
CEO, KPN Telecom

地球正朝着工具性（instrumented）、互连性（interconnected）与智慧性（intelligence）的方向发展。

欢迎来到充满无尽机会的新大陆… *智慧的地球*

全球化以及在全球范围内提供的资源

实时接入信息流

数十亿移动设备访问万维网

新技术
新复杂性
新风险

全新协作方式

这些新机会伴随着新风险

新兴技术

- 虚拟化和云计算
- 依赖于IT的物理基础架构
- 应用是容易发生安全违规和安全攻击事件的薄弱点

数据和信息量激增

- 数据量每隔18个月翻一番
- 围绕着信息上下文的存储、安全和发现技术变得越来越重要

无线世界

- 移动平台发展成为全新的身份识别方法
- 与用于保护PC的安全相比，安全技术落后多年

供应链

- 供应链的安全级别与最薄弱的链路相同… 合作伙伴需要承担制度遵从风险并且对故障负责

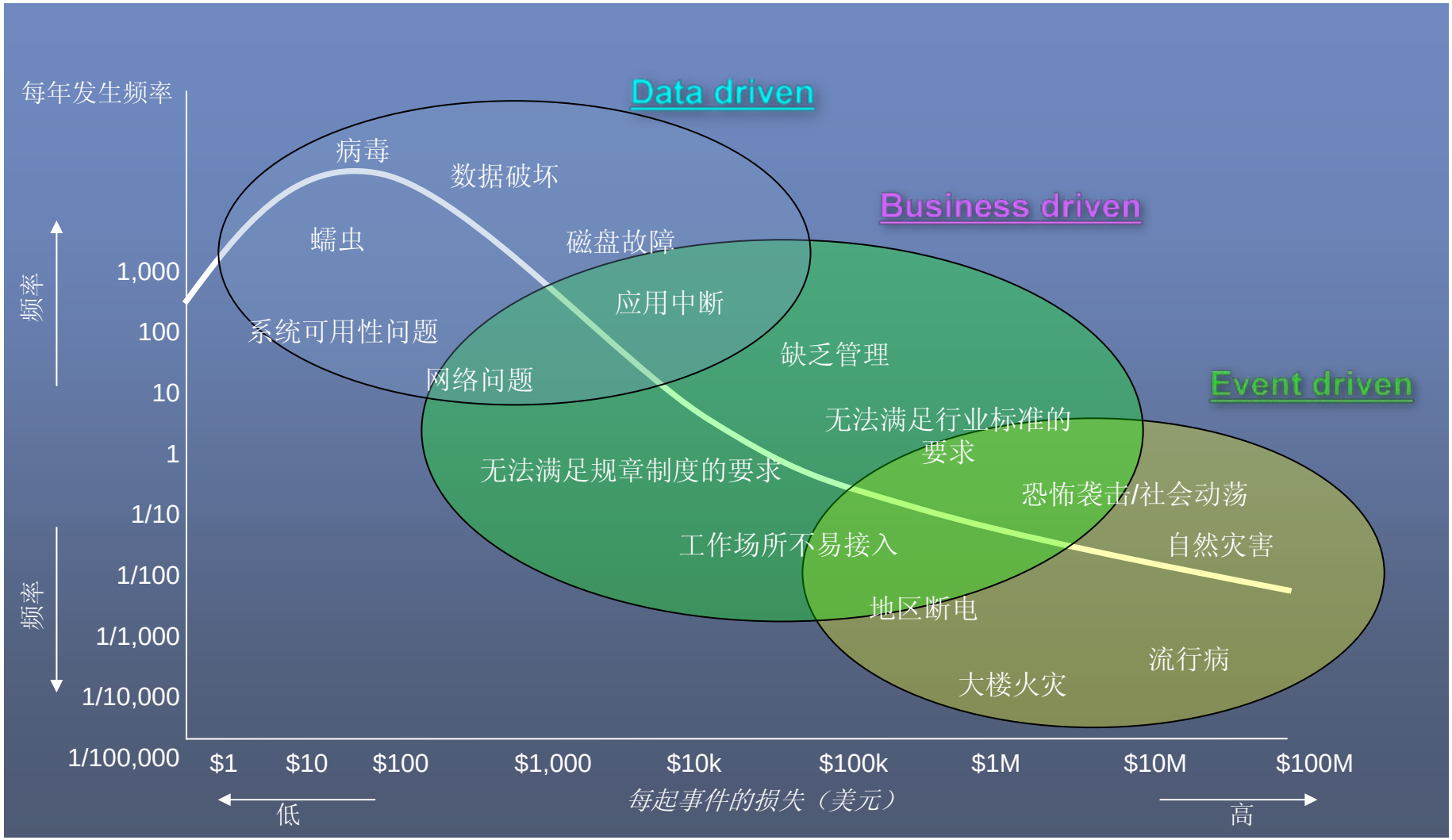
公众希望不被打扰

- 将安全性集成到基础架构、流程和应用中，是渴望，或是期望

制度遵从挑战

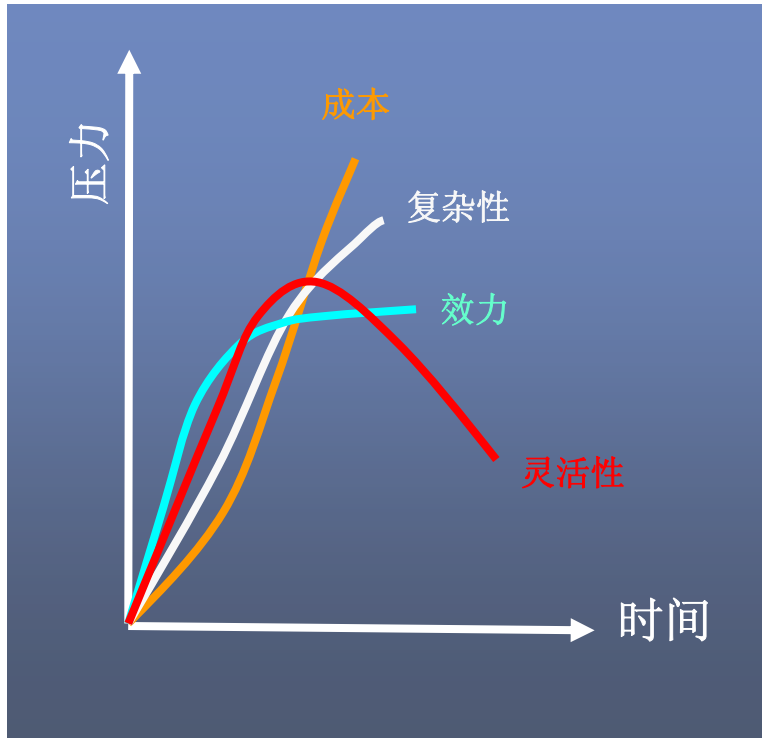
- 公司试图在安全性与制度遵从投资之间维持均衡

并非所有的风险都拥有相同系数



单点产品不是完整的安全解决方案…

- 在安全性与成本之间找到均衡点
  - 公理是… 永远不要为了保护一匹价值10美元的马匹而去搭建100美元的篱笆（得不偿失）
- 研究表明，帕累托法则（80-20规则）适用于IT安全性*
  - 经证实，**87%**的安全违规事件都可通过合理的控制得到避免*
- 少量投资关键安全控制工具，将实现巨大的成效
  - 关键控制工具能够帮助企业解决各级风险问题
  - 使用关键安全控制工具的机构，绩效远远高于及其他机构*



*来源：W.H. Baker, C.D. Hylender, J.A. Valentine, 2008数据违规调查报告, Verizon Business, 06/2008
ITPI: IT Process Institute, EMA 12/2008

企业普遍存在的安全问题

重建设 轻运维

- 安全管理、运行上还没有建立起定位清晰、有效的角色和流程体系
- 忽略监视安全产品运行状况
- 安全产品种类多，没有措施或机制保证选对安全产品，并持续发挥作用
- 有安全系统管理日志系统，对日志缺乏有效的审计
- 缺少有效手段对安全事件进行及时的、有效的处理
- 安全事件管理（包括紧急响应）流程和制度不够完善，缺少足够的技术手段来支持流程和制度

重IT安全 轻信息安全

- 能意识到安全问题，有部分安全控制，但安全没有深入到软件开发的生命周期
- 注重防火墙、入侵检测等基础设施的建设，缺乏关注数据泄漏、内部误用滥用
- 片面注重组网安全，物理隔离

家底不清

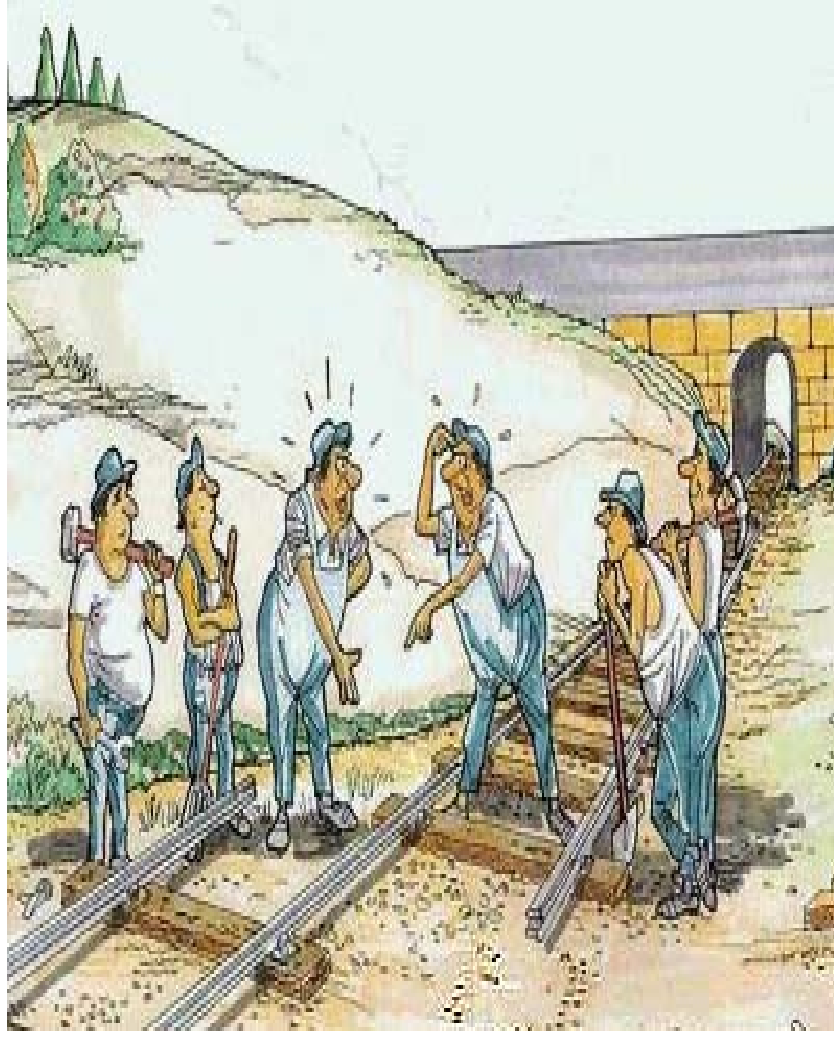
- 不能掌握企业安全弱点，不能有效评价企业安全风险状况；
- 企业安全需求不明，建设方向不清

重后台 轻用户

- 员工信息安全意识薄弱，导致企业内部非授权访问、越权访问、网络滥用，以及病毒蠕虫等问题严重
- 终端安全仅重视产品部署，没有形成完整的防护体系

如果欠缺某些环节，真正的安全体系就无法建立

- 如何简化风险管理流程 ，重新评估工作优先级，以便在挑战不断变化的形势下更好地控制风险
- 如何有效控制风险，简化安全风险的生命周期
- 如何建立完整的安全框架和解决方案组合，利用创新和集成来构建完整的安全管理和技术保障体系
- 如何与业务流程保持一致，以确保持续改进



企业信息安全框架V5.0

安全治理、风险管理和合规

- 战略和治理框架
- 风险管理框架
- 合规和策略遵从

安全运维

- 安全事件监控
- 安全事件响应
- 安全事件审计
- 安全策略管理
- 安全绩效管理
- 安全外包服务

基础安全服务和架构

物理安全

- 机房安全
- 视频监控安全

基础架构安全

- 网络安全
- 主机安全
- 终端安全

应用安全

- 应用开发生命周期安全
- 业务流程安全
- Web应用安全
- 应用开发环境安全

数据安全

- 数据生命周期管理
- 数据泄露保护
- 数据加密
- 数据归档
- 灾难备份

身份/访问安全

- 身份验证
- 访问管理
- 身份生命周期管理

建议企业制定的信息安全框架

Security Principle (安全原则)
描述信息安全的业务需求价值

Security Policy (安全政策)
描述信息安全的目地、方向、愿景及责任

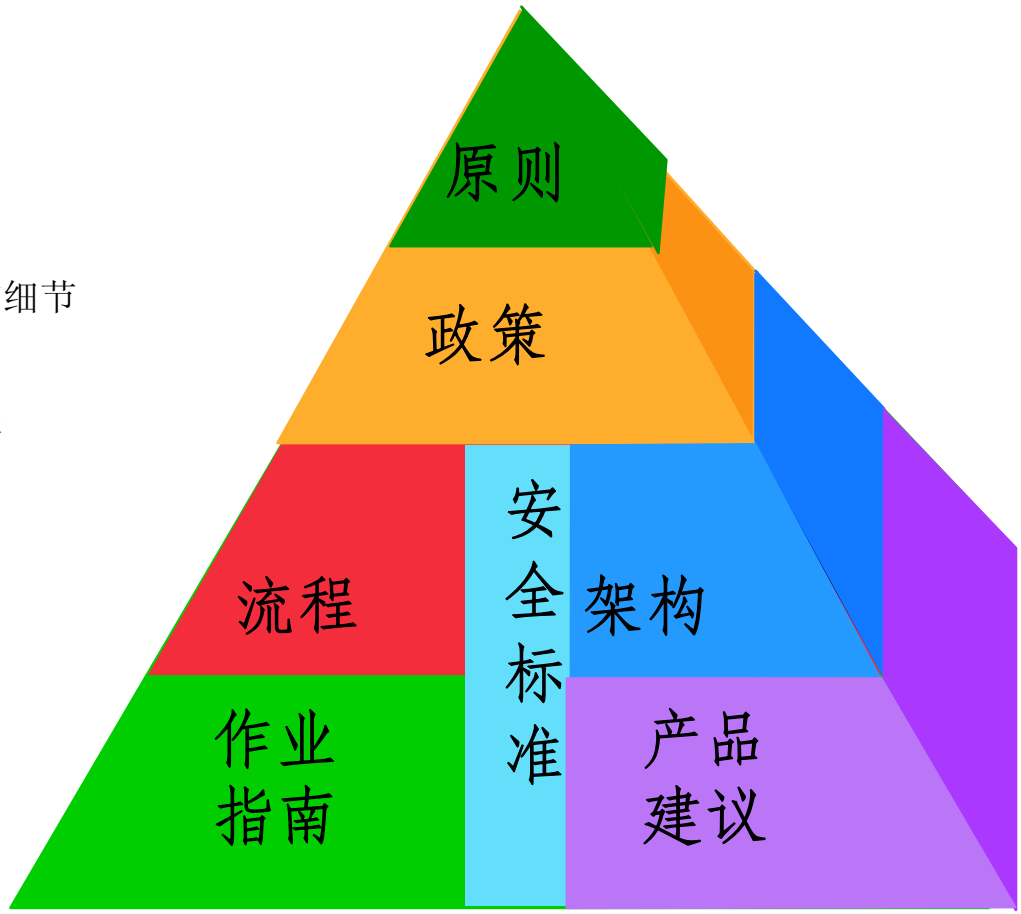
Security Standard (安全标准)
信息安全实施规则，包括技术、方法及其它细节

Security Process (安全流程)
于跨部门实施政策标准的活动、工作及程序

Security Procedures (安全作业指南)
描述个人在流程上的详细工作

Security Architecture (安全架构)
信息安全技术如何结合的细节

Security Products (安全产品)
信息安全解决方案所选的产品及工具

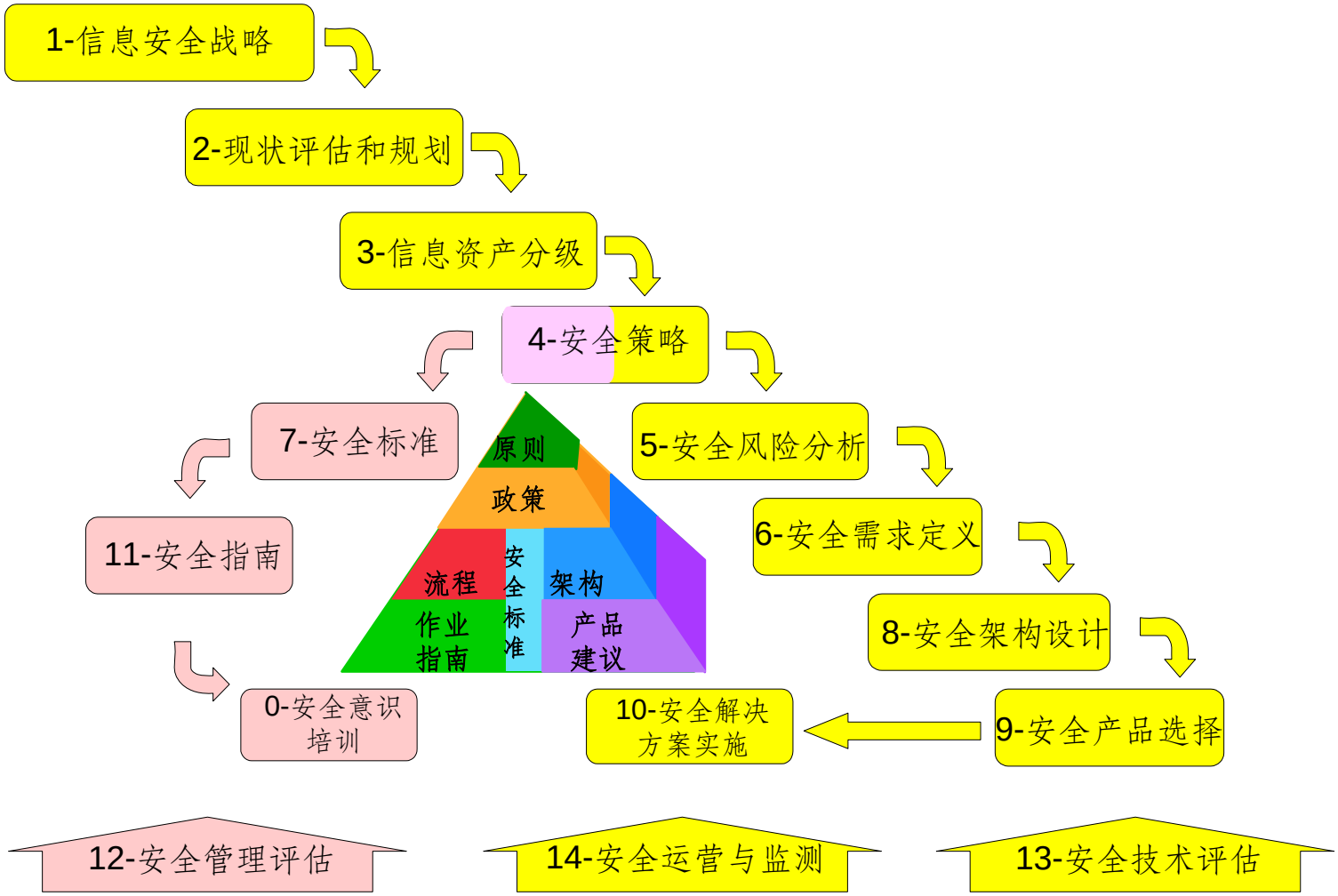


我们从哪里起步？

- 身份和接入管理
- 加密和密钥管理
- 数据保护
- 版本管理
- 变化和配置管理
- 威胁和安全漏洞管理
- 问题和事故管理
- 安全信息和事件管理

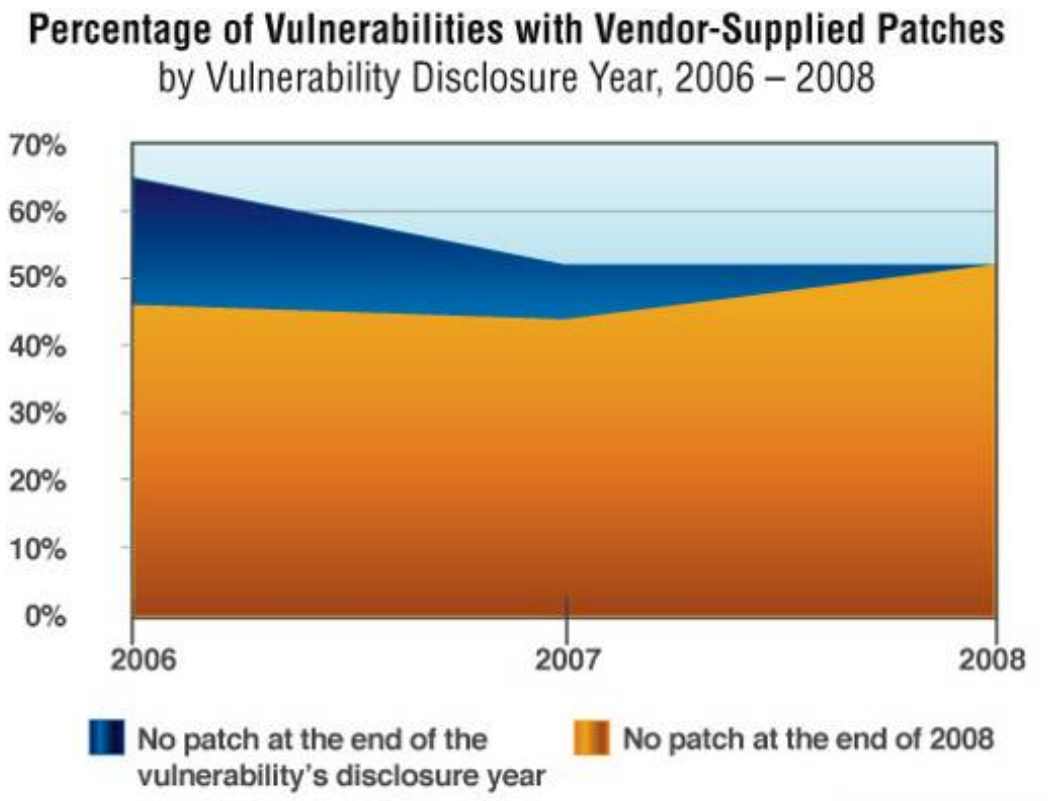
- 使用成熟度评估模型，跨越所有的IT安全领域去了解您的安全就绪性
- 在安全性与投资之间找到均衡点
- 开发有先后之分的安全路线图

IBM 的企业信息安全建设路线图



厂商没有为安全漏洞提供补丁

- 在2008年披露的所有安全漏洞中，53%的漏洞厂商没有提供修复补丁
  - 44%在2007年发现的安全漏洞以及46%在2006年发现的安全漏洞，至今仍不存在补丁



威胁演进

Threats and Protection – First 20 Years

New Era Threats with Legacy Defense

For the past 20 years, signature AV systems protected enterprises from most attacks. However, threats today are more heavily armed, multi-faceted, and can be deployed more strategically to bypass legacy protection systems.

黑客入侵、病毒、蠕虫、僵尸程序、间谍软件、钓鱼攻击、特洛伊木马、DOS/DDos、网络爬虫、零天攻击...

漏洞利用攻击的经济学

- 安全行业必须学会在制订安全响应程序时考虑到犯罪动机
- 经济利益（成本和收益）是安全漏洞利用攻击的最大动机
- 严重安全漏洞可能并不像表面上那样严重
- 您必须在投资和安全漏洞攻击成本与机
- 会之间进行认真权衡

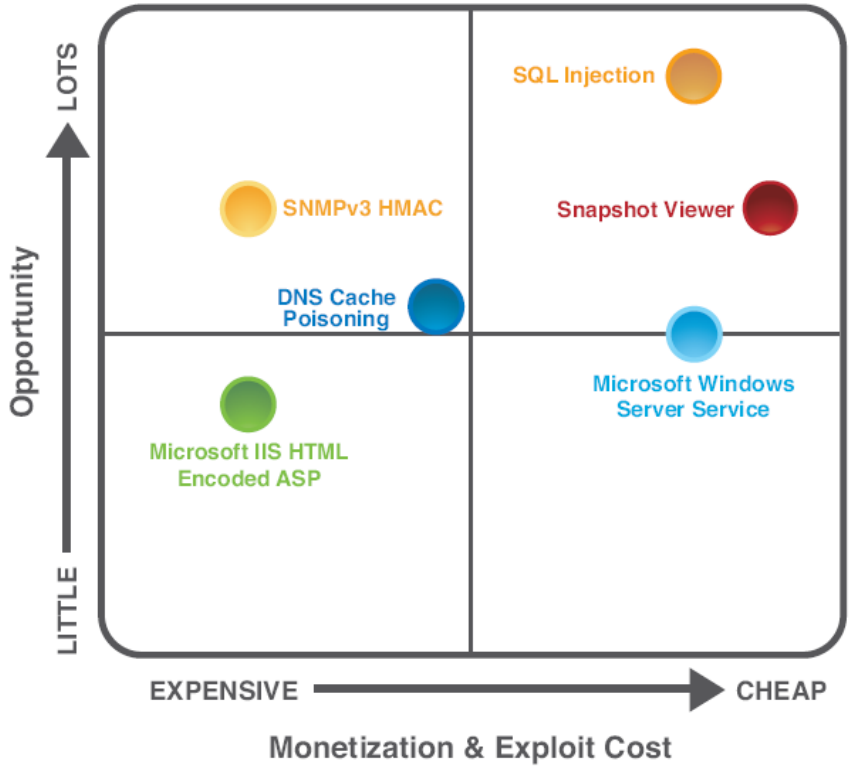


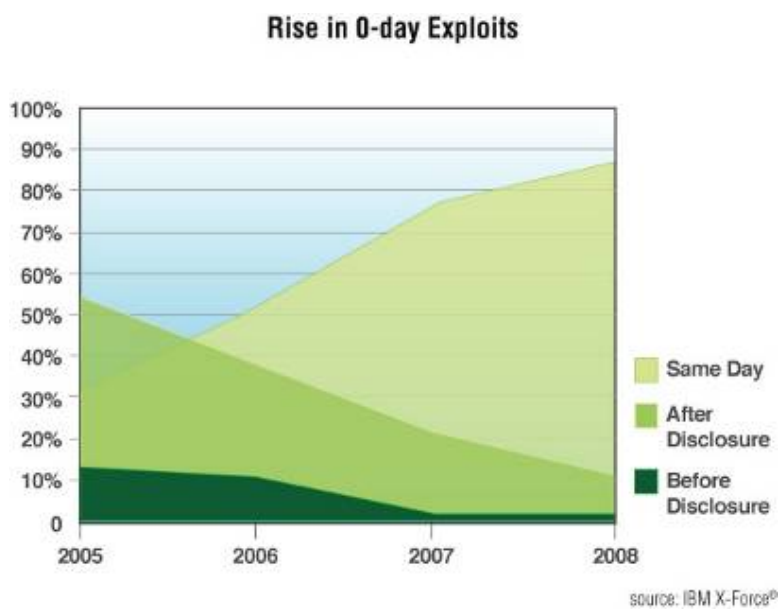
Figure 7: Exploitability Probability Quadrant

黑客可在工具的帮助下轻松发动安全漏洞利用攻击

- 黑客可利用现成的安全漏洞利用工具包和易用的管理界面
  - 没有人知道在已安装的工具包中，有多少是买来的，有多少是租来的或盗来的
- 2008年，89%的公共安全漏洞利用攻击都发生在官方披露安全漏洞当天甚至之前
  - 比2007年的79%有所增加

Most Popular Exploit Toolkits (2H 2008)

Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	mPack (and variants)	CuteQQ
2.	CuteQQ	AdM
3.	AdM	mPack (and variants)
4.	FirePack	Neosploit
5.	Neosploit	Tornado (and variants)



Most Popular Exploits

Rank	2008 (Full Year)	2008 H2 (Second Half)
1.	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2.	RealPlayer IERPCtl ActiveX (CVE-2007-5601)	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)
3.	Apple QuickTime RSTP URL (CVE-2007-0015)	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)
4.	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	RealPlayer IERPCtl ActiveX (CVE-2007-5601)
5.	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Apple QuickTime RSTP URL (CVE-2007-0015)

最终用户的认知趋势 – 及早防范！

Attack vs. Best Practice	
Spoofed Email	• Don't view emails from unknown parties
Malicious attachments	• Don't click on .exe, .com, .scr, etc.
Emotional appeals	• Beware of random emails making big promises
URL spoofing, obfuscation	• *Don't trust any solicitations*
Drive-by Malware	• *Don't trust anything from anyone, anywhere*

IBM ISS™ X-Force®研发中心的使命是：

- 调查并评估威胁和保护问题
- 开发新技术，以便迎接未来的安全挑战
- 提供安全保护，解决现在的问题
- 为媒体和用户团体提供培训

X-Force研发中心推动IBM ISS安全创新

研究 → 技术 → 解决方案

X-Force 保护引擎

- 现有引擎的扩展
- 新保护引擎的创建

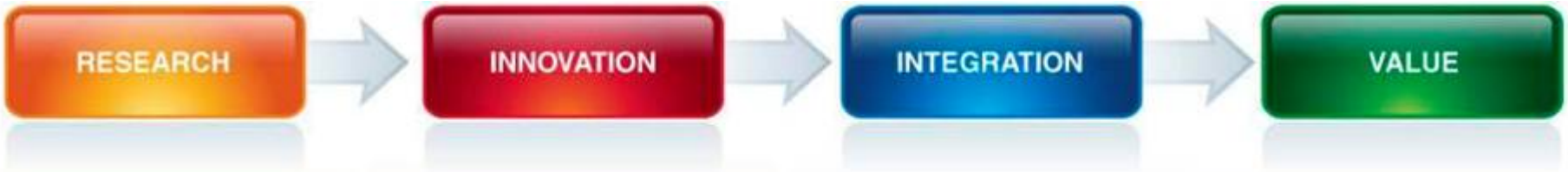
X-Force XPU's

- 安全内容更新技术的最新发展
- 安全内容更新技术QA

X-Force 智库

- X-Force数据库
- 馈送信息的监控与收集
- 情报共享

创建商业价值的关键 – IBM与众不同之处



- **X-Force研发中心**
- **高级威胁数据库**
- **知识库**
  - 日处理20亿起事件
  - 2,500名客户
  - 数千个设备

- **前瞻性技术**
- **可扩展、自适应**
  - 不断发展的威胁形态
  - 动态的业务需求
- **高可扩展的解决方案**
- **多种交付模式可供选择**
  - 产品和服务解决方案

- **自动补救**
- **安全的业务解决方案**
- **自动策略管理**
- **工作流集成**
- **生命周期管理**
- **一体化解决方案(如接入)**
- **客户选择 =控制**

- **同时满足安全性和制度遵从需求(控制)**
- **IT效率**
- **业务效率**
- **预防威胁！**
- **提供保证防护的服务等级协议（SLA）**
- **以业务价值为中心，不是以威胁管理为中心**
  - 降低成本
  - 降低复杂性

IBM ISS真正创造价值 –降低总体拥有成本（TCO）

IBM安全研究协作机构

8家安全运行中心 + 9家安全研发中心 + 监控133个国家 + 签约保护超过2万多个设备 + 全球拥有3,700多名MSS客户 + 每日处理超过40亿起事件

IBM拥有无与伦比的全球和地方经验，

能够提供完整的解决方案 – 并且管理安全性的成本和复杂性

IBM互联网安全系统保护平台

有史以来最高级、最完整的安全架构 —提供前瞻式安全

- 集成安全智能
- 全套的专业安全服务
- 平台和服务可扩展性
- 多种数据源的关联与集成
- “一流”的基础产品
- **24/7**外包安全管理
- 延长系统运行时间并提高系统性能，无需巨额投资技术或资源

保护平台

安全治理、风险管理和合规

- 企业安全战略规划服务
- ISO27001认证指导咨询服务
- 信息安全管理体系培训服务
- 安全管理差距分析服务
- 信息安全管理体系咨询及设计服务
- 企业信息系统风险评估服务
- PCI DSS合规遵从服务
- 信息安全等级保护合规遵从服务

安全运维

- 安全运维管理中心设计及建设服务
- 安全运维管理平台规划及建设服务
- 安全策略的开发及制定服务
- 安全事件响应流程设计服务
- 安全应急响应服务
- 安全绩效考核体系设计
- 安全事件审计咨询服务
- 安全事件审计平台的规划及建设服务
- 操作行为审计平台规划及建设服务
- 管理安全服务

基础安全服务和架构

物理安全

- 机房物理安全评估服务
- 机房物理安全设计服务
- 智能视频监控平台建设服务

基础架构安全

- 基础架构安全评估服务
- 网络入侵防护系统
- 统一威胁管理系统
- 脆弱性管理系统
- 网络安全加固服务
- 主机入侵防护系统
- 主机访问控制系统
- 主机系统加固服务
- 终端安全控制系统

应用安全

- 应用开发生命周期安全评估和设计服务
- 应用系统代码审计服务
- 渗透测试服务
- 应用安全规范设计服务
- 应用安全评测服务
- 网页防篡改服务
- Web应用渗透测试及评估
- 应用开发环境安全评估及建设服务

数据安全

- 数据生命周期安全评估服务
- 数据安全管理规范设计服务
- 数据安全保护系统集成服务
- 数据敏感性分析服务
- 数据防丢失集成服务
- 数据加密保护服务
- 数据归档设计及实施服务
- 信息系统灾难恢复的规划及实施

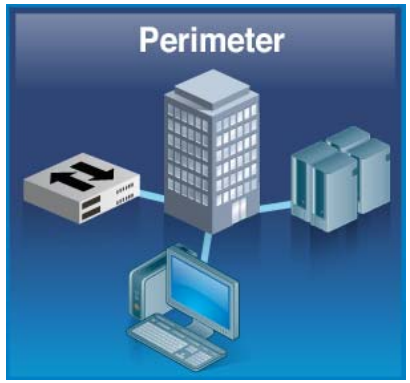
身份/访问安全

- 统一身份及访问管理架构设计服务
- 统一身份及访问管理平台建设服务
- 强身份认证集成服务
- 应用系统身份及访问管理平台整合服务
- 企业单点登录(ESSO)集成服务
- 统一身份及访问管理帐号清理服务
- 统一身份及访问管理帐号管理流程设计及实施服务

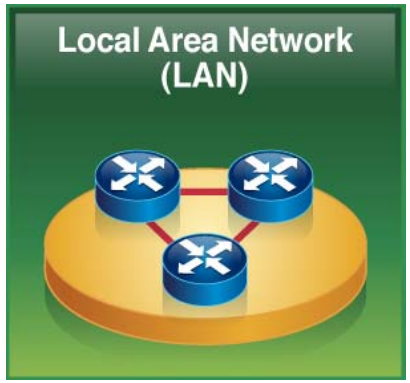
举例说明 – IBM端到端的集成安全产品

一流的安全技术，降低成本和复杂性

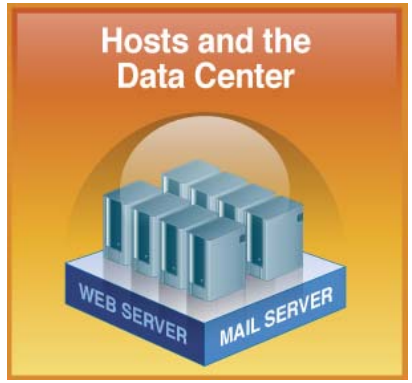
- **MSS市场领导者**
- 解决方案能够帮助客户在风险和保护之间实现完美均衡
- 利用业界最佳业务实践和一流的安全技术/服务
- 帮助评估并实施的安全控制工具，借此解决制度遵从问题



- 入侵防御
- 防火墙
- 统一威胁管理
- 用户身份识别
- 访问控制
- 安全事件和日志管理

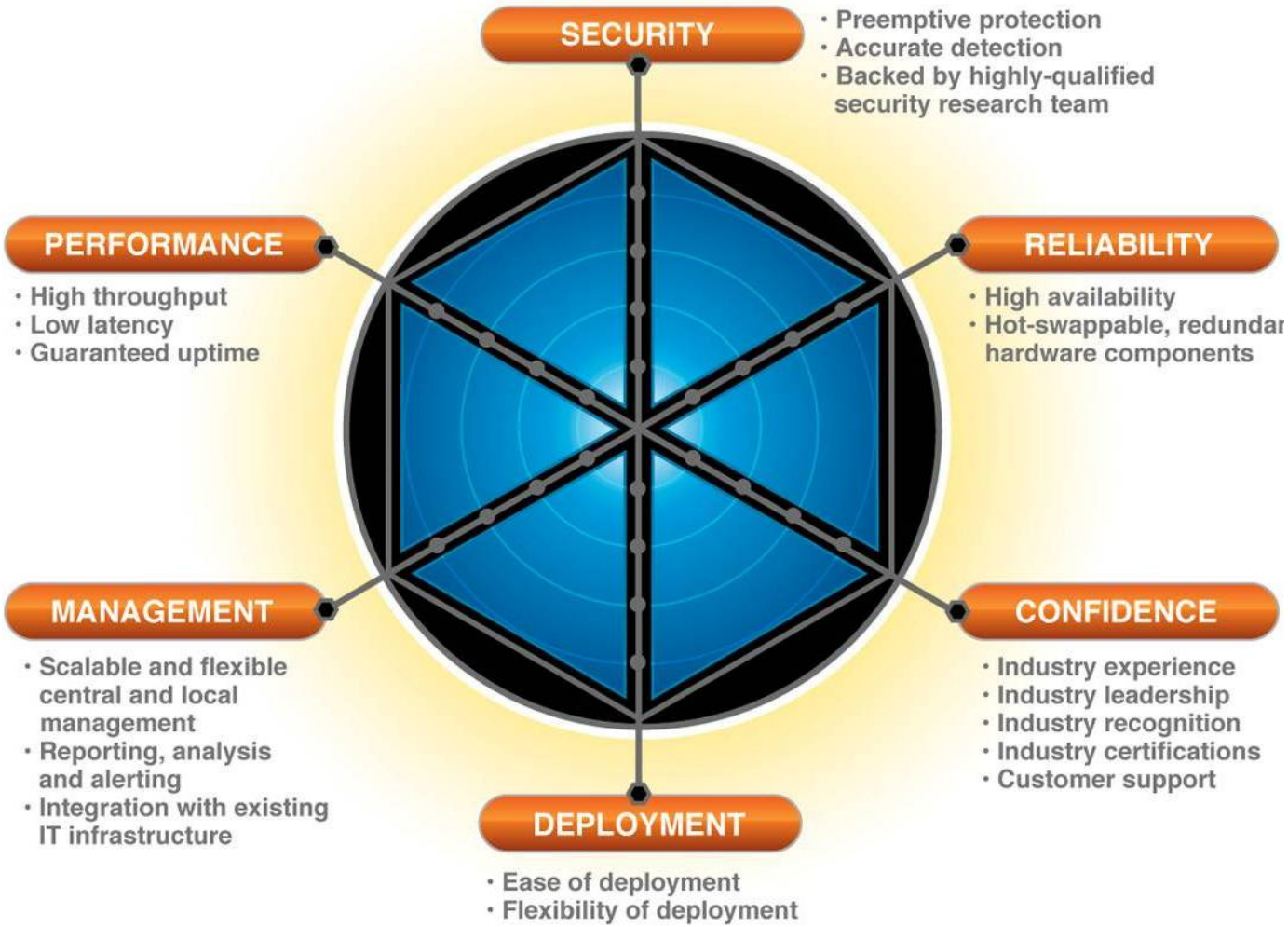


- 入侵防御
- 安全漏洞管理和防御
- 修复
- 安全事件和日志管理

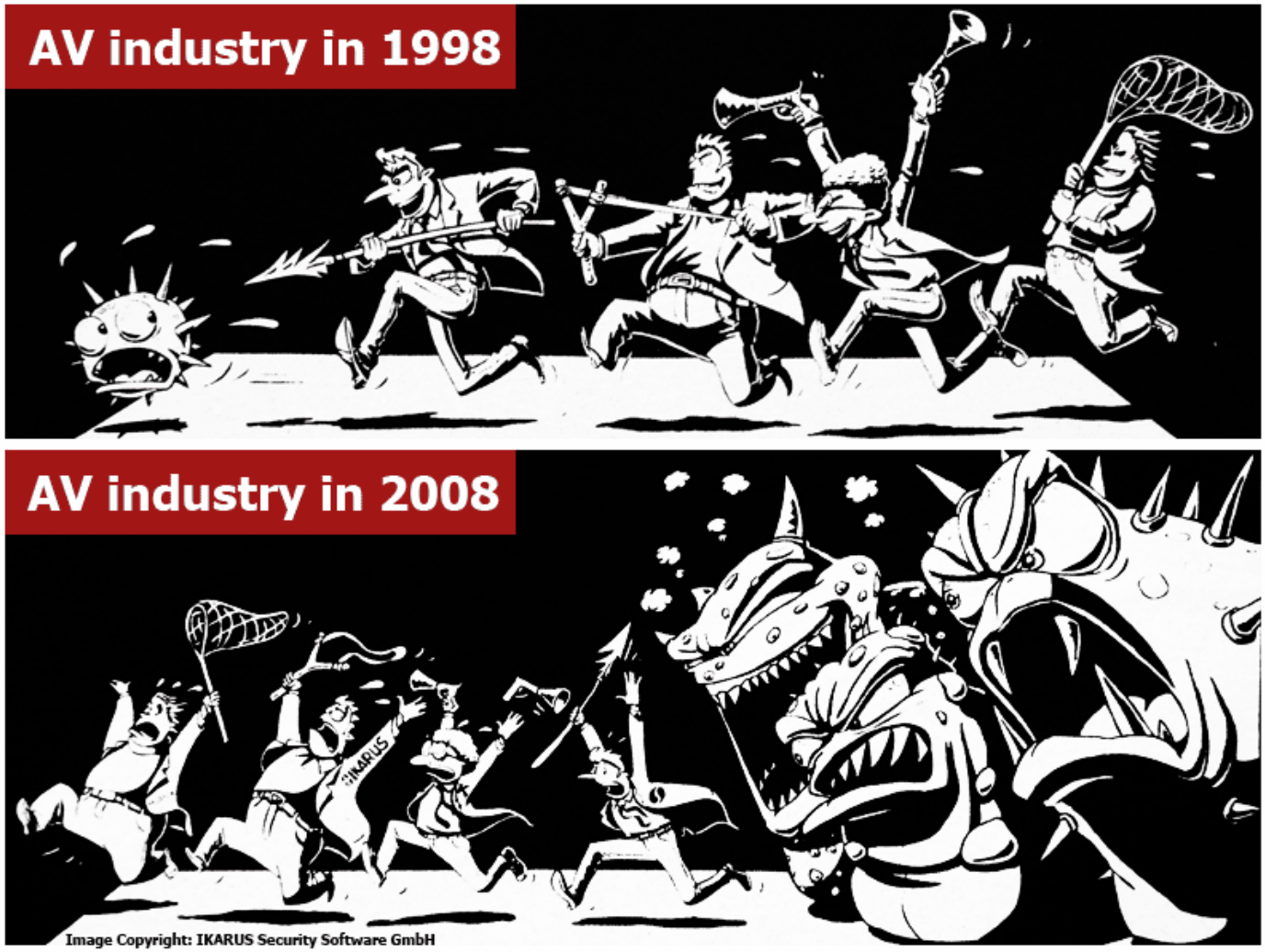


- 主机保护(服务器和桌面系统)
- 消息传递和Web安全性
- 安全漏洞管理
- 数据安全性
- 安全事件和日志管理

如何选择有效的安全产品？



恶意软件变脸


AV industry in 1998
AV industry in 2008
IKARUS
Image Copyright: IKARUS Security Software GmbH


以安全之浆
撑发展之船


Thank
You